

16

October 14, 2003

Ms. Jennifer J. Johnson, Secretary  
Board of Governors of the  
Federal Reserve System  
20<sup>th</sup> Street and Constitution Ave., NW  
Washington, DC 20551  
Docket No. OP-1155

Public Information Room  
Office of the Comptroller  
of the Currency  
250 E Street, SW Mail Stop I-5  
Washington, DC 20219  
Docket No. 03-18

Robert E. Feldman, Executive Secretary  
Attention: Comments/OES  
Federal Deposit Insurance Corporation  
550 17<sup>th</sup> Street, NW  
Washington, DC 20429

Regulation Comments, Chief Counsel's Office  
Office of Thrift Supervision  
1700 G Street, NW  
Washington, DC 20552  
Attention: No. 2003-35

Dear Sirs and Madams:

Compass Bank appreciates the opportunity to comment on the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice. Compass Bank is the lead bank subsidiary of Compass Bancshares, Inc., a \$25.6 billion Southwestern financial holding company which operates 358 full-service banking offices in Texas, Alabama, Florida, Arizona, Colorado and New Mexico.

Compass strongly supports the federal government's efforts to combat identity theft and financial fraud, and commends the Agencies for their efforts in interpreting the provisions of section 501(b) of the Gramm-Leach-Bliley Act.

In the August 12 Notice relating to the Guidance, comments were requested on all aspects of the proposed Guidance and specifically on (1) whether the appropriate standard has been set for requiring customer notice and (2) the potential burden associated with the customer notice provisions. We will address the broad provisions set forth in the Guidance, along with the specific issues above, in this letter.

#### **General Comments**

While we acknowledge the Agencies' responsibility to issue Guidance to effect the safeguards prescribed in section 501(b) of the Gramm-Leach-Bliley Act, Compass Bank does not support the response program requirements as set forth for the following reasons:

- We believe that, as a rule, financial institutions already notify customers when fraud is likely, regardless of cause. For example, it is common practice in the industry today

for banks to notify charge card customers and replace their cards in the event a merchant's card system security is breached.

- As a practical matter, the proposed Guidance requires notification when fraud or identity theft is merely possible; this would result in little customer benefit and, in fact, needlessly alarm customers where little likelihood of harm exists, resulting in significant unnecessary inconvenience to consumers.
- The proposed Guidance defines as "sensitive information" information that, in reality, is readily available on the Internet or routinely disclosed by the customer to effect transactions.
- We believe that the Agencies have grossly underestimated the costs associated with the requirements; that these additional costs of compliance will be passed on to customers; and that the public would be better served if those resources were employed to improve the ability of financial institutions to prevent fraud and identity theft.

Therefore, *we strongly urge the Agencies to withdraw the proposed Guidance.*

Instead, we encourage the Agencies to focus their collective efforts on measures to prevent and detect fraud and identity theft such as (1) improved methods of customer identification, (2) industry adoption of superior technological tools, e.g., smart cards and fraud detection systems, (3) protection of information on public networks such as the Internet, and (4) systems for sharing fraud and identity theft information among institutions and law enforcement Agencies.

If the Agencies choose to refine and issue this Guidance, our concerns, comments, requests for clarifications, and recommendations for improving the Guidance are set forth below.

#### **Standard Triggering Notification**

The standard triggering notification is unclear and biased towards notification in the absence of certainty. Specifically, notification is required "unless the institution... reasonably concludes that misuse of the information is unlikely to occur...." This appears to impose on the institution an affirmative duty to determine that fraud (misuse) is unlikely and, therefore, requires customer notification when such a positive conclusion cannot be reached. In the absence of a positive likelihood of misuse, notification will almost certainly result in unnecessary customer inconvenience. Therefore, we believe that the standard should require notification only when there is a positive likelihood of misuse in the reasonable estimation of the institution.

#### **Sensitive Customer Information**

The definition of sensitive information includes information routinely disclosed by the customer in order to execute transactions, such as name and account number. We believe that it is inappropriate to require financial institutions to treat information routinely disclosed by customers as "sensitive."

Of the items deemed "sensitive information" in the proposed Guidance, exclusive of access codes and PINs, only the social security number is not routinely disclosed by customers when transacting business. While the perception that social security numbers are "secret" is common among the public, recent news articles (e.g., see CNN.COM, Thursday, August 28, 2003, "Social Security Numbers Sold On Web") have demonstrated that social security numbers are widely available. In fact, online "skip trace" services return both the social security number and date of birth when provided only a name and address. We are not suggesting that financial institutions should treat social security numbers as public data; however, they are not secret and we believe that the Guidance should not treat them as such.

### **Content of Notice**

The key elements of notice required by the Guidance are unnecessarily prescriptive and may not be appropriate in all circumstances. We request that the Agencies change the language to make clear that the contents of the notice should be appropriate to the nature of the information disclosed.

In some cases, elements of notice required by the Guidance are simply incorrect. For example, the Guidance requires that customers be advised that "the institution will assist the customer to correct and update information in any consumer report relating to the customer, as required by the Fair Credit Reporting Act." FCRA requires only that institutions correct any erroneous information provided by the institution. We request that the Agencies remove the incorrect language.

While we appreciate the Agencies' efforts to outline all possible considerations, we are concerned that the "optional elements" of notification will become de facto standards, thereby requiring financial institutions to justify not including them. We, therefore, request that the "optional elements" section be deleted.

### **Delivery of Notice**

The Guidance states that the notice may be "delivered in any manner that will ensure that the customer is likely to receive it." The Agencies then specifically mention mail, telephone, and electronic delivery. However, we believe that there are circumstances where direct customer notification is an unreasonable burden. We request that the Guidance be revised to permit indirect notification procedures such as newspaper, television, and radio notices, where appropriate or necessary.

### **Notification Under Direction**

In the Background section, the Agencies state that, "as in other circumstances, the Agencies also expect financial institutions to notify customers upon the direction of the institution's primary Federal regulator." We are unaware of the existing "other circumstances" to which the Agencies refer and are unclear what form such direction would take. The Agencies' authority to order notification of customers must also be set forth by statute. We ask the Agencies to clarify the comment and describe the process and form of such direction and their authority to order such notice.

### **Estimate of Burden on Institution**

We appreciate the difficulty of estimating the future costs of the proposed requirements. In reaching an occurrence rate of 2% of institutions per year, the Agencies reference an FDIC study in a footnote but do not provide a source for review. Therefore, we do not know whether the study was recent, representative of the population of financial institutions generally, and used a definition of "unauthorized access to customer information" that corresponds to this Guidance. However, in our experience and as confirmed by discussions in industry associations, insider fraud, including data harvesting by organized criminals, is clearly increasing and we would expect larger institutions to experience several instances of unauthorized use of customer information each year. We are aware that other large institutions have similar expectations and must conclude that the 2% rate is grossly understated, as described in the next paragraph.

In addition, we believe that the Agencies have significantly underestimated the probable costs associated with each occurrence. The estimated time to produce notices does not appear to include time to write computer programs to extract data and format reports. It does not include the approximately \$0.60 per customer for a one-page letter, envelope, and first class postage. It does not include the customer service time handling the enormous number of calls prompted by receiving the notice, nor the costs associated with closing/reopening accounts (an obvious customer reaction), printing new checks or embossing new cards, etc. The printing and mailing costs, alone, for one notice to our customer database at the current postal rates would be at least \$500,000.

### **Significant Burden on Customers Ignored by Guidance**

The Agencies fail to adequately consider the burden and distress to customers who would begin receiving numerous notices of "unauthorized access" to their data. For most institutions, access for the purpose of viewing one record on a database is access to all records and there is no way of tracing every record actually viewed. The Agencies' regulation is so broad that anytime there is unauthorized access to a database, for whatever reason, the financial institution would be required to notify all customers with records in that database that their account information may have been viewed by an unauthorized person. The stress to customers of having to change account numbers, change passwords, monitor their credit reports, etc., is enormous and may be totally unnecessary. An example of unauthorized access that should not trigger notification is as follows: an employee of the financial institution who is not authorized to access account records, gains access to the database containing his ex-wife's account in order to prove that she is receiving more income than disclosed in a child support proceeding. In this case, the financial institution can reasonably draw the conclusion that the risks of access to customer records other than the records of the ex-wife are small to non-existent. The financial institution has no way of knowing, however, whether that employee accessed any other records in the database. Under the Guidance, as now written, therefore, the financial institution has to give notice to all of its customers that their accounts were subject to unauthorized access.

We believe that the Agencies should reassess the estimated economic impact of the proposed regulation and consider carefully whether it is justified given the questionable customer benefit.

**Conclusion**

Compass Bank strongly urges the Agencies to revise the initial Guidance based on the responses received from this and other institutions, and we request that any revised version of the Guidance be circulated for comment. We appreciate the opportunity to respond to the Agencies' notice and commend the Agencies on their efforts to fight consumer identity theft. We trust that the Agencies will carefully consider whether the proposed Guidance effectively furthers this goal.

Yours truly,

Phyllis M. Gamble  
Vice President and Senior Risk Advisor